UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,199	02/14/2002	Adrian Filipi-Martin	CHM03	3201

7590 09/08/2005

McNair Law Firm, P.A.
P.O. Box 10827
Greenville, SC 29603

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/076,199	FILIPI-MARTIN ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 are pending.

Claim Objections

2. Claim 10 is objected to because of the following informalities: On page 27, line 5 the term should read "that" instead of "than". Appropriate correction is required.

3. Claim 19 is objected to because of the following informalities: On page 29, line 19, the term should read "with" instead of "wit". Appropriate correction is required.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Meffert et al. (Pub No. 2003/0037261)

Referring to the rejection of claim 1, Meffert et al. discloses an automated encryption system for encrypting an electronic message from a sender to a recipient comprising:

a computer readable medium (See Page 8, Section 0088)

a network port in communication with the computer readable medium for accessing a set of public key data having a public key associated with the recipient (See Page 6, Section 0072)

a set of computer readable encryption instructions embodied in the computer readable medium for:

receiving the electronic message from the sender addressed to the recipient (See Page 6, Section 0072)

retrieving the public key associated with the recipient from the public key data via the network connection (See Page 6, Section 0076)

encrypting the electronic message according to the public key associated with the recipient (See Page 6, Section 0076)

and forwarding the encrypted message to the recipient for subsequent retrieval so that the electronic message is automatically encrypted and delivered to the recipient (See Page 8, Section 0089)

Referring to the rejection of claim 2, Meffert et al. discloses the claimed limitation wherein a set of private key data embodied in the computer readable medium having a private key associated with the sender (See Page 8, Section 0088, Page 6, Section 0072)

and the set of computer readable encryption instructions include instructions for:

retrieving the private key associated with the sender from the set of private key data (See Page 6, Section 0076)

and signing the electronic message from the sender according to the private key associated with the sender so that the recipient can verify the authenticity of the electronic message (See Page 6, Section 0076)

Referring to the rejection of claim 3, Meffert et al. discloses the claimed limitation wherein a set of private key data contained within the computer readable medium having a private key associated with the sender (See Page 8, Section 0088, Page 6, Section 0072)

and a set of computer readable access instructions embodied in the computer readable medium for:

receiving an access attempt input from the sender (See Page 9, Section 0093)

retrieving the private key associated with the sender from the set of private data (See Page 9, Section 0098)

validating the access attempt input according to the private key to determine whether a valid access attempt input has been provided (See Page 9, Section 0098)

and encrypting the electronic message according to the public key if the access attempt input is valid so that only senders with valid access attempt inputs may send encrypted messages (See Page 9, Section 0098)

Referring to the rejection of claim 4, Meffert et al. discloses the claimed limitation wherein the set of computer readable access instructions include instructions for signing the electronic message using the private key associated with the sender so that the electronic message can be authenticated (See Page 13, Section 0137)

Referring to the rejection of claim 5, Meffert et al. discloses the claimed limitation wherein a set of private key data contained within the computer readable medium (See Page 8, Section 0088, Page 9, Section 0101)

a set of computer readable key maintenance instruction embodied within the computer readable medium for:

creating a key pair having the at least one public key associated with the senders (See Page 6, Section 0072)

a private key associated with the public key and the sender (See Page 6, Section 0076)

storing the public key within the set of public key data so that the public key associated with the sender is available for retrieval (See Page 6, Section 0075)

storing the private key within the private key data so that the sender can retrieve the private key for decrypting message sent to the sender (See Page 6, Section 0076, Page 7, Section 0077)

and deleting the key pair to prevent the sender from decrypting encrypted messages so that an automated key management system is provided for automatically managing key pairs for senders (See Page 7, Section 0078)

Referring to the rejection of claim 6, Meffert et al. discloses the claimed limitation wherein a set of public key data embodied within the computer readable medium (See Page 6, Section 0072)

Referring to the rejection of claim 7, Meffert et al. discloses the claimed limitation wherein a set of encrypted private key data contained within the computer readable medium (See Page 8, Section 0088, Page 9, Section 0101)

a set of computer readable key maintenance instruction embodied within the computer readable medium for:

creating a key pair having the at least one public key associated with the sender and a private key associated with the public key and the sender (See Page 6, Section 0072)

storing the public key within the set of public key data so that the public key associated with the sender is available for retrieval (See Page 6, Section 0075)

receiving a password from the sender (See Page 7, Section 0081)

encrypting the private key according to the password (See Page 7, Section 0081)

storing the encrypted private key within the private key data so that the sender can retrieve the private key for decrypting message sent to the sender (See Page 6, Section 0076, Page 7, Section 0077)

and deleting the key pair to prevent the sender from decrypting encrypted messages so that an automated key management system is provided for automatically managing key pairs for senders (See Page 7, Section 0078)

Referring to the rejection of claims 8 and 19, Meffert et al. discloses an automated encryption system for decrypting an electronic message from a sender to a recipient comprising:

a computer readable medium (See Page 8, Section 0088)

a set of computer readable decryption instructions embodied in the computer readable medium for:

receiving the electronic message from the sender addressed to the recipient (See Page 6, Sections 0072,0074)

retrieving the private key associated with the recipient from the set of private key data (See Page 8, Section 0085)

decrypting the electronic message according to the private key (See Page 8, Section 0085)

and providing the decrypted message to the recipient so that the recipient automatically retrieves and decrypts an electronic encrypted message without manually managing private keys (See Page 8, Section 0085)

Referring to the rejection of claim 9, Meffert et al. discloses the claimed limitation wherein a network port in communication with the computer readable medium for accessing a set of public key data having a public key associated with the sender (See Page 6, Section 0072)

a set of computer readable encryption instructions embodied in the computer readable medium for:

receiving the encrypted message having a digital signature associated with the sender (See Page 6, Section 0075)

retrieving the public key associated from the sender from the digital signature (See Page 6, Section 0076)

validating the electronic message according to the digital signature to provide validation information (See Page 6, Section 0076)

and providing the resulting validation information to the recipient so that the recipient can be notified as to the authenticity of the received encrypted message (See Page 7, Section 0078)

Referring to the rejection of claim 10, Meffert et al. discloses the claimed limitation wherein a network port in communication with the computer readable medium for accessing a set of public key data having a public key data (See Page 8, Section 0088, Page 9, Section 0101)

a set of computer readable key maintenance instruction embodied within the computer readable medium for:

creating a key pair having a public key associated with the recipient (See Page 6, Section 0072)

storing the public key within the set of public key data via the network port (See Page 6, Section 0075)

storing the private key within the private key data (See Page 6, Section 0076, Page 7, Section 0077)

and deleting the key pair to prevent the recipient from decrypting messages so that an automated key management system is provided for automatically managing key pairs for recipients (See Page 7, Section 0078)

Referring to the rejection of claim 11, Meffert et al. discloses the claimed limitation wherein a set of public key data embodied within the computer readable medium (See Page 6, Section 0072)

Referring to the rejection of claim 12, Meffert et al. discloses the claimed limitation wherein the set of computer readable maintenance instructions include instruction for:

receiving a password from the sender (See Page 9, Section 0098)

and encrypting the private key associated with the sender so that the private key can not be used to decrypt messages without supplying an access attempt matching the password (See Page 10, Section 0111)

Referring to the rejection of claim 13, Meffert et al. discloses an computerized system for encrypting an electronic message from a sender to a recipient comprising:

a computer readable medium (See Page 8, Section 0088)

a means for receiving an electronic message from a sender to a recipient embodied in the computer readable medium (See Page 6, Section 0072)

a means for obtaining a public key associated with the recipient (See Page 6, Section 0072)

a means for encrypting the electronic message according to the public key (See Page 6, Section 0076)

and a means for forwarding the encrypted electronic message to the recipient for subsequent decryption and retrieval (See Page 8, Section 0089)

Referring to the rejection of claim 14, Meffert et al. discloses the claimed limitation wherein an encrypted private key associated with the sender encrypted according to a password supplied to the sender and contained within the computer readable medium (See Page 8, Section 0088, Page 9, Section 0101)

a means for receiving an access attempt from the sender (See Page 9, Section 0093)

and a means for validating the access attempt according to the encrypted private key so that the electronic message is not encrypted unless the access attempt is valid (See Page 7, Section 0081)

Referring to the rejection of claim 15, Meffert et al. discloses the claimed limitation wherein a means for informing the sender that the public key associated with the recipient cannot be found so that electronic message cannot be encrypted (See Page 9, Sections 0093-0094)

and a means for sending the electronic message to the recipient (See Page 9, Section 0095)

Referring to the rejection of claim 16, Meffert et al. discloses the claimed limitation wherein a computer readable medium (See Page 8, Section 0088)

a means for receiving an encrypted electronic message from the sender to the recipient (See Page 6, Sections 0072,0074)

a means for obtaining a private key associated with the recipient (See Page 6, Section 0076)

a means for decrypting the encrypted electronic message from the sender to the recipient so that the recipient can receive and decrypt an encrypted message (See Page 7, Section 0081)

Referring to the rejection of claim 17, Meffert et al. discloses the claimed limitation wherein a digital signature associated with the sender contained within the computer readable medium (See Page 6, Section 0075)

and a means for signing the electronic message with the digital signature (See Page 13, Section 0137)

Referring to the rejection of claim 18, Meffert et al. discloses the claimed limitation wherein a means for receiving an electronic message having a digital signature associated with the sender (See Page 8, Section 0088, Page 6, Section 0072)

and a means for verifying the authenticity of the electronic message according to the digital signature so that the recipient is ensured that the electronic message truly originates from the sender (See Page 6, Section 0076)

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Srinivasan (Pub No. 2003/0126085) discloses a system and method for dynamic authentication of electronic messages using a digital certificate. Meffert et al. (Pub No. 2002/0059144) discloses a system and method for automatically implementing PKI-based encryption between recipient and sender.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-

272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CDS

cdf
September 2, 2005

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137